

Remarks on 2-q-bit states

Berthold-Georg Englert^{1,2} and Nasser Metwally³

¹Max-Planck-Institut für Quantenoptik
Hans-Kopfermann-Strasse 1
85748 Garching, Germany

²Abteilung für Quantenphysik
Universität Ulm
Albert-Einstein-Allee 1
89081 Ulm, Germany

³Sektion Physik
Universität München
Theresienstraße 37
80333 München, Germany

17 July 2000

Abstract

We distinguish six classes of families of locally equivalent states in a straightforward scheme for classifying all 2-q-bit states; four of the classes consist of two subclasses each. The simple criteria that we stated recently for checking a given state's positivity and separability are justified, and we discuss some important properties of Lewenstein-Sanpera decompositions. An upper bound is conjectured for the sum of the degree of separability of a 2-q-bit state and its concurrence.

PACS: 89.70.+c, 03.65.Bz

1 Introduction

Entangled q-bits (binary quantum alternatives) are exploited in most schemes proposed for quantum communication purposes, for quantum information processing, or for the secure key distribution procedures known as quantum cryptography. The basic units are entangled q-bit pairs. Obviously then, a thorough understanding of the properties of 2-q-bit states is desirable. Although there has been considerable progress in this matter recently, the situation is still quite unsatisfactory.

The characterization of the 2-q-bit states produced by some source requires the experimental determination of 15 real parameters. Ideally, this is done by measuring a suitably chosen set of five observables [1] that constitute “a complete set of five pairs of complementary propositions” [2]. In an optical model [3], which makes use of single-photon 2-q-bit states, these measurements can be

realized, and other experimental studies of 2-q-bit states can be performed as well.

Then, based on the knowledge of the 15 state-specifying parameters, one can classify the 2-q-bit state. We distinguish, in Sec. 2, six classes of families of locally equivalent states. Roughly speaking, local equivalence means that the difference is of a geometrical, not a physical nature. In a certain sense, the 15 parameters can be regarded as consisting of 6 geometrical ones and 9 physical ones.

The classification of Sec. 2 is straightforward but not sufficient. One also needs to know if the 2-q-bit state in question is useful for quantum communication purposes. In the technical terms of Sec. 4, we ask for its degree of separability as a numerical measure for this usefulness. The degree of separability is part and parcel of the so-called optimal Lewenstein-Sanpera decomposition [4] of a 2-q-bit state. This decomposition is known for a number of relevant types of states [5] but, despite a good understanding of its properties, presently we do not have a method for finding it for any arbitrary 2-q-bit state.

In Sec. 5 we remark briefly on the so-called concurrence of a 2-q-bit state [6, 7] and surmise that the sum of the degree of separability and the concurrence does not exceed unity. The Appendix reports some technical details.

2 Families of 2-q-bit states

We employ the terminology and the notational conventions of [5]. As usual, we describe the individual q-bits with the aid of analogs of Pauli's spin vector operator: $\vec{\sigma}$ for the first q-bit, $\vec{\tau}$ for the second. These row vectors refer to two three-dimensional vector spaces that are unrelated, which is to say that in

$$\begin{aligned}\vec{\sigma} &= \sum_{\alpha=x,y,z} \sigma_{\alpha} \vec{e}_{\alpha} = (\sigma_x, \sigma_y, \sigma_z) \begin{pmatrix} \vec{e}_x \\ \vec{e}_y \\ \vec{e}_z \end{pmatrix}, \\ \vec{\tau} &= \sum_{\beta=x,y,z} \tau_{\beta} \vec{n}_{\beta} = (\tau_x, \tau_y, \tau_z) \begin{pmatrix} \vec{n}_x \\ \vec{n}_y \\ \vec{n}_z \end{pmatrix}\end{aligned}\tag{1}$$

the orthonormal right-handed vector sets $\vec{e}_x, \vec{e}_y, \vec{e}_z$ and $\vec{n}_x, \vec{n}_y, \vec{n}_z$ have nothing to do with each other.

In addition to these pre-chosen xyz coordinate systems, we'll also consider 123 coordinate systems that are adapted to the 2-q-bit state of interest. Then

$$\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) \begin{pmatrix} \vec{e}_1 \\ \vec{e}_2 \\ \vec{e}_3 \end{pmatrix}, \quad \vec{\tau} = (\tau_1, \tau_2, \tau_3) \begin{pmatrix} \vec{n}_1 \\ \vec{n}_2 \\ \vec{n}_3 \end{pmatrix}\tag{2}$$

are the respective parameterizations of $\vec{\sigma}$ and $\vec{\tau}$. As an elementary illustration think of the statistical operator of the first q-bit, specified by the Pauli vector

$$\vec{s} = \langle \vec{\sigma} \rangle,$$

$$\begin{aligned} \rho_1 &= \frac{1}{2}(1 + \vec{s} \cdot \sigma^\downarrow) = \frac{1}{2}(1 + s_x \sigma_x + s_y \sigma_y + s_z \sigma_z) \\ &= \frac{1}{2}(1 + s \sigma_1), \end{aligned} \quad (3)$$

where $s \geq 0$ is the length of \vec{s} and the 123 system has \vec{e}_1 in the direction of \vec{s} by definition. Note that we are carefully distinguishing row vectors from column vectors, as in the scalar product $\vec{s} \cdot \sigma^\downarrow$ of row \vec{s} and column σ^\downarrow ; of course, columns and rows are transposes of each other, $s^\downarrow = \vec{s}^T$. Admittedly, this distinction is somewhat pedantic, but it makes book keeping much easier.

Unitary transformations that affect only one of the q-bits or both q-bits independently are *local* transformations. Geometrically speaking, local transformations rotate $\vec{\sigma}$ and $\vec{\tau}$. Two states that can be turned into each other by a local transformation are *locally equivalent*. For instance, two first-q-bit states (3) are equivalent if their Pauli vectors have the same length; at most the two states can differ by the direction of \vec{e}_1 . In other words: The difference of two equivalent states is only in the 123 bases that go with the generic form $\frac{1}{2}(1 + s \sigma_1)$.

Likewise, there are families of locally equivalent 2-q-bit states. To decide whether two given 2-q-bit states belong to the same family, one may put them into a generic form that is uniquely fixed by convenient conventions. The following set of conventions seems to be quite natural.

It all begins with recalling that the general form of a 2-q-bit state is given by

$$P = \frac{1}{4} \left(1 + \vec{\sigma} \cdot s^\downarrow + \vec{t} \cdot \tau^\downarrow + \vec{\sigma} \cdot \overleftrightarrow{C} \cdot \tau^\downarrow \right). \quad (4)$$

It involves the cross dyadic \overleftrightarrow{C} ,

$$\overleftrightarrow{C} = \langle \sigma^\downarrow \vec{\tau} \rangle = (e_x^\downarrow, e_y^\downarrow, e_z^\downarrow) \begin{pmatrix} C_{xx} & C_{xy} & C_{xz} \\ C_{yx} & C_{yy} & C_{yz} \\ C_{zx} & C_{zy} & C_{zz} \end{pmatrix} \begin{pmatrix} \vec{n}_x \\ \vec{n}_y \\ \vec{n}_z \end{pmatrix}, \quad (5)$$

in addition to the Pauli vectors s^\downarrow and \vec{t} ,

$$\begin{aligned} s^\downarrow &= \langle \sigma^\downarrow \rangle = (e_x^\downarrow, e_y^\downarrow, e_z^\downarrow) \begin{pmatrix} s_x \\ s_y \\ s_z \end{pmatrix}, \\ \vec{t} &= \langle \vec{\tau} \rangle = (t_x, t_y, t_z) \begin{pmatrix} \vec{n}_x \\ \vec{n}_y \\ \vec{n}_z \end{pmatrix}. \end{aligned} \quad (6)$$

In a first step we bring \overleftrightarrow{C} into the diagonal form

$$\overleftrightarrow{C} = \pm (e_1^\downarrow c_1 \vec{n}_1 + e_2^\downarrow c_2 \vec{n}_2 + e_3^\downarrow c_3 \vec{n}_3)$$

$$\text{for } \begin{cases} \det \left\{ \overleftarrow{C} \right\} \geq 0, \\ \det \left\{ \overleftarrow{C} \right\} < 0, \end{cases} \quad (7)$$

with its characteristic values ordered in accordance with

$$c_1 \geq c_2 \geq c_3 \geq 0. \quad (8)$$

Their squares are the eigenvalues of $\overleftarrow{C} \cdot \overleftarrow{C}^T$ or $\overleftarrow{C}^T \cdot \overleftarrow{C}$; the eigencolumns of $\overleftarrow{C} \cdot \overleftarrow{C}^T$ constitute the orthonormal right-handed set $e_1^\downarrow, e_2^\downarrow, e_3^\downarrow$, and the corresponding $\vec{n}_1, \vec{n}_2, \vec{n}_3$ are eigenrows of $\overleftarrow{C}^T \cdot \overleftarrow{C}$.

Whereas the sign in (7) and the values of the c_k s are determined by the three local invariants¹

$$\text{Sp} \left\{ \overleftarrow{C}^T \cdot \overleftarrow{C} \right\}, \quad \det \left\{ \overleftarrow{C} \right\}, \quad \text{Sp} \left\{ \left(\overleftarrow{C}^T \cdot \overleftarrow{C} \right)^2 \right\}, \quad (9)$$

the 123 bases are not uniquely specified by (7), however, because the simultaneous replacements

$$(e_1^\downarrow, e_2^\downarrow, e_3^\downarrow) \rightarrow (-e_1^\downarrow, -e_2^\downarrow, e_3^\downarrow), \quad \begin{pmatrix} \vec{n}_1 \\ \vec{n}_2 \\ \vec{n}_3 \end{pmatrix} \rightarrow \begin{pmatrix} -\vec{n}_1 \\ -\vec{n}_2 \\ \vec{n}_3 \end{pmatrix}, \quad (10)$$

for example, do not change the right-hand side of (7). The resulting freedom in choosing $e_1^\downarrow, e_2^\downarrow, e_3^\downarrow$ (which then fixes $\vec{n}_1, \vec{n}_2, \vec{n}_3$ unless $c_2 = 0$) is then used to enforce conventions imposed on the coefficients in

$$\begin{aligned} s^\downarrow &= \langle \sigma^\downarrow \rangle = (e_1^\downarrow, e_2^\downarrow, e_3^\downarrow) \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix}, \\ \vec{t} &= \langle \vec{\tau} \rangle = (t_1, t_2, t_3) \begin{pmatrix} \vec{n}_1 \\ \vec{n}_2 \\ \vec{n}_3 \end{pmatrix}. \end{aligned} \quad (11)$$

In brief terms, these conventions aim at making as many of the s_k s and t_k s vanish as possible and to give definite signs to as many as possible of the remaining ones. Eventually, each family is characterized by nine numbers: the values of the three local invariants in (9), the three s_k ($k = 1, 2, 3$) coefficients, and the three t_k s, some of them equal to zero and others with a known sign. Roughly speaking, of the 15 coefficients appearing in (5) and (6), six are thus used up in defining the two 123 coordinate systems, and nine to identify the family of

¹We write $\text{Sp} \{ \}$ for the trace of a dyadic in order to avoid confusion with quantum mechanical traces such as $C_{xy} = \langle \sigma_x \tau_y \rangle = \text{Tr} \{ \sigma_x \tau_y P \}$.

locally equivalent states to which the given P belongs. Clearly, the nine family-defining parameters are invariant under local transformations.

Degeneracy among the characteristic values of the cross dyadic distinguishes six classes of families,

$$\begin{aligned}
c_1 = c_2 = c_3 = 0: & \quad \text{class A ,} \\
c_1 = c_2 = c_3 > 0: & \quad \text{class B ,} \\
c_1 > c_2 = c_3 = 0: & \quad \text{class C ,} \\
c_1 > c_2 = c_3 > 0: & \quad \text{class D ,} \\
c_1 = c_2 > c_3: & \quad \text{class E ,} \\
c_1 > c_2 > c_3: & \quad \text{class F .}
\end{aligned} \tag{12}$$

In classes A and C the + sign in (7) applies; both signs can occur in classes B, D, E, and F which, therefore, consist of two subclasses each.

Given the local invariants of (9), we find the respective class as follows. First calculate the auxiliary quantities

$$\begin{aligned}
a &= \frac{9}{4} \text{Sp} \left\{ \overleftarrow{C}^T \cdot \overleftarrow{C} \right\} \text{Sp} \left\{ \left(\overleftarrow{C}^T \cdot \overleftarrow{C} \right)^2 \right\} \\
&\quad - \frac{5}{4} \left[\text{Sp} \left\{ \overleftarrow{C}^T \cdot \overleftarrow{C} \right\} \right]^3 + \frac{27}{2} \left[\det \left\{ \overleftarrow{C} \right\} \right]^2, \\
b &= \frac{3}{2} \text{Sp} \left\{ \left(\overleftarrow{C}^T \cdot \overleftarrow{C} \right)^2 \right\} - \frac{1}{2} \left[\text{Sp} \left\{ \overleftarrow{C}^T \cdot \overleftarrow{C} \right\} \right]^2,
\end{aligned} \tag{13}$$

which are subject to $a^2 \leq b^3$. Then we have the classification

$$\begin{aligned}
\text{class A} & \quad \text{if} \quad a^2 = b^3 = 0 \quad \text{and} \quad \det \left\{ \overleftarrow{C} \right\} = 0, \\
\text{class B} & \quad \text{if} \quad a^2 = b^3 = 0 \quad \text{and} \quad \det \left\{ \overleftarrow{C} \right\} \neq 0, \\
\text{class C} & \quad \text{if} \quad a^2 = b^3 > 0 \quad \text{and} \quad a > 0 \\
& \quad \quad \quad \text{and} \quad \det \left\{ \overleftarrow{C} \right\} = 0, \\
\text{class D} & \quad \text{if} \quad a^2 = b^3 > 0 \quad \text{and} \quad a > 0 \\
& \quad \quad \quad \text{and} \quad \det \left\{ \overleftarrow{C} \right\} \neq 0, \\
\text{class E} & \quad \text{if} \quad a^2 = b^3 > 0 \quad \text{and} \quad a < 0, \\
\text{class F} & \quad \text{if} \quad a^2 < b^3.
\end{aligned} \tag{14}$$

The generic forms for the various classes are as follows.

Class A: Since $\overleftarrow{C} = 0$ here, we can choose the two sets of 123 coordinates independently, and $s_1 \geq 0$, $s_2 = s_3 = 0$ as well as $t_1 \geq 0$, $t_2 = t_3 = 0$ specify the conventions. This class consists of a two-parametric set of families of the generic form

$$P = \frac{1}{4} (1 + s\sigma_1 + t\tau_1) \quad \text{with} \quad s \geq 0, \quad t \geq 0. \tag{15}$$

For $s = 0, t = 0$ we have the chaotic state $P_{\text{chaos}} = \frac{1}{4}$ which forms a single-state family all by itself.

Class B: Here we can choose $e_1^\downarrow, e_2^\downarrow, e_3^\downarrow$ freely and the conventional choice is specified by

$$s^\downarrow = e_1^\downarrow s, \quad \vec{t} = t_1 \vec{n}_1 + t_3 \vec{n}_3$$

$$\text{with } \left\{ \begin{array}{cc} s > 0 & \text{and } t_3 \geq 0 \\ \text{or} \\ s = 0 & \text{and } t_1 = t \geq 0, t_3 = 0 \end{array} \right\}. \quad (16)$$

Each subclass $[\pm \text{ in (7)}]$ consists of four-parametric sets of families. In passing we note that the so-called Werner states constitute the two class-B families with $s = 0$ and $t = 0$.

Class C: Here the replacement (10) is used to enforce $s_1 \geq 0$ or $t_1 \geq 0$ if $s_1 = 0$. Then $s_2 = 0, s_3 \geq 0$ and $t_2 = 0, t_3 \geq 0$ are achieved by suitable rotations of $e_2^\downarrow, e_3^\downarrow$ and, independently, of \vec{n}_2, \vec{n}_3 . In summary, this establishes

$$s^\downarrow = e_1^\downarrow s_1 + e_3^\downarrow s_3, \quad \vec{t} = t_1 \vec{n}_1 + t_3 \vec{n}_3,$$

$$\vec{C} = e_1^\downarrow c_1 \vec{n}_1$$

$$\text{with } \left\{ \begin{array}{cc} s_1 \geq 0 \\ \text{or} \\ s_1 = 0 & \text{and } t_1 \geq 0 \end{array} \right\}$$

$$\text{and } s_3 \geq 0, t_3 \geq 0 \quad (17)$$

for the five-parametric sets of families.

Class D: In distinction from class C, the rotations in the 23 sectors are not independent here. Thus we get

$$s^\downarrow = e_1^\downarrow s_1 + e_3^\downarrow s_3, \quad \vec{t} = t_1 \vec{n}_1 + t_2 \vec{n}_2 + t_3 \vec{n}_3,$$

$$\vec{C} = \pm (e_1^\downarrow c_1 \vec{n}_1 + e_2^\downarrow c_2 \vec{n}_2 + e_3^\downarrow c_3 \vec{n}_3)$$

$$\text{with } \left\{ \begin{array}{cc} s_1 \geq 0 \\ \text{or} \\ s_1 = 0 & \text{and } t_1 \geq 0 \end{array} \right\}$$

$$\text{and } \left\{ \begin{array}{cc} s_3 \geq 0 & \text{and } t_2 \geq 0 \\ \text{or} \\ s_3 = 0 & \text{and } t_2 = 0, t_3 \geq 0 \end{array} \right\}. \quad (18)$$

Each subclass contains seven-parametric sets of families.

Class E: This class is very similar to class D, but now the degeneracy is in the 12 sector, and so we have

$$s^\downarrow = e_1^\downarrow s_1 + e_3^\downarrow s_3, \quad \vec{t} = t_1 \vec{n}_1 + t_2 \vec{n}_2 + t_3 \vec{n}_3,$$

$$\begin{aligned}
\vec{C} &= \pm (e_1^\downarrow c_1 \vec{n}_1 + e_2^\downarrow c_1 \vec{n}_2 + e_3^\downarrow c_3 \vec{n}_3) \\
\text{with } &\left\{ \begin{array}{c} s_1 \geq 0 \quad \text{and} \quad t_2 \geq 0 \\ \text{or} \\ s_1 = 0 \quad \text{and} \quad t_1 \geq 0, \quad t_2 = 0 \end{array} \right\} \\
\text{and } &\left\{ \begin{array}{c} s_3 \geq 0 \\ \text{or} \\ s_3 = 0 \quad \text{and} \quad t_3 \geq 0 \end{array} \right\}. \tag{19}
\end{aligned}$$

Here, too, each subclass is made up of seven-parametric sets of families.

Class F: The lack of degeneracy limits changes of the 123 bases to discrete 180° rotations as in (10) where the rotation is around the 3rd axes. The generic form is then defined by that choice of 123 coordinates for which as many as possible of the coefficients $s_1, t_1, s_2, t_2, s_3, t_3$, are non-negative (in this order, say). Here we get, in each subclass, sets of families specified by the full number of nine parameters, of which five or more are non-negative.

Arbitrary local unitary transformations turn members of a family into other members of the same family — this, we recall, is the defining property of a family of locally equivalent states. It is possible that some local transformations have no effect at all, as exemplified by $U_{\text{loc}} = \exp(i\varphi\sigma_1 + i\phi\tau_1)$ acting on the class-A state (15). Therefore, some families are larger than others, and determining a family's size is a problem of considerable interest. Recent progress on this front is reported by Kuś and Życzkowski [8].

We close this section with a single example. Pure states are of the generic form

$$\begin{aligned}
P_{\text{pure}} &= \frac{1}{4} (1 + p\sigma_1 - p\tau_1 - \sigma_1\tau_1 - q\sigma_2\tau_2 - q\sigma_3\tau_3) \\
\text{with } &0 \leq p \leq 1, \quad q = \sqrt{1 - p^2} \geq 0. \tag{20}
\end{aligned}$$

One verifies easily the purity condition

$$P_{\text{pure}} (1 - P_{\text{pure}}) = 0. \tag{21}$$

For $p = 0, q = 1$ we have the family of Bell states,

$$P_{\text{Bell}} = \frac{1}{4} (1 - \sigma_1\tau_1 - \sigma_2\tau_2 - \sigma_3\tau_3), \tag{22}$$

which is in class B; the $p = 1, q = 0$ family consists of the product states $\frac{1}{2}(1 + \sigma_1)\frac{1}{2}(1 - \tau_1)$ and is in class C; and the $0 < p < 1$ families belong to class D. These families are of different sizes [8]: three-dimensional, four-dimensional, and five-dimensional, respectively.

3 Positivity and separability

An arbitrary choice for the (real) coefficients in (1) and (5) or, equivalently, of the nine family-defining parameters plus the 123 coordinate systems specifies

a hermitian P of unit trace, but its positivity must be ensured by imposing restrictions on the Pauli vectors s^\downarrow , \vec{t} , and the cross dyadic \overleftrightarrow{C} . It is expedient to switch the emphasis from P to the traceless operator K introduced by

$$P = \frac{1}{4}(1 - K), \quad K = 1 - 4P, \quad (23)$$

so that $P \geq 0$ requires

$$K \leq 1. \quad (24)$$

Convex sums of two states are weighted sums of their K s. Admixing P_{chaos} to a given P amounts to multiplying its K by a factor.

One could, of course, check the positivity criterion (24) by calculating the eigenvalues of K . For such purposes, it is often very convenient to use a 4×4 -matrix representation in which $\sigma_{1,2,3}$ and $\tau_{1,2,3}$ have imaginary antisymmetric matrices,

$$\begin{aligned} & \vec{\sigma} \cdot s^\downarrow + \vec{t} \cdot \tau^\downarrow \\ & \cong \begin{pmatrix} 0 & -i(s_1 + t_1) & +i(s_2 + t_2) & -i(s_3 - t_3) \\ +i(s_1 + t_1) & 0 & +i(s_3 + t_3) & +i(s_2 - t_2) \\ -i(s_2 + t_2) & -i(s_3 + t_3) & 0 & +i(s_1 - t_1) \\ +i(s_3 - t_3) & -i(s_2 - t_2) & -i(s_1 - t_1) & 0 \end{pmatrix}, \end{aligned} \quad (25)$$

and products $\sigma_j \tau_k$ ($j, k = 1, 2, 3$) have real symmetric matrices, in particular

$$\begin{aligned} & \vec{\sigma} \cdot \overleftrightarrow{C} \cdot t^\downarrow = \pm \sum_{k=1}^3 \sigma_k c_k \tau_k \\ & \cong \pm \begin{pmatrix} c_1 + c_2 - c_3 & 0 & 0 & 0 \\ 0 & c_1 - c_2 + c_3 & 0 & 0 \\ 0 & 0 & -c_1 + c_2 + c_3 & 0 \\ 0 & 0 & 0 & -c_1 - c_2 - c_3 \end{pmatrix} \end{aligned} \quad (26)$$

is diagonal. But precise knowledge of the actual eigenvalues of K is not needed if we only want to verify (24).

Since K is traceless, its eigenvalues κ_j ($j = 1, 2, 3, 4$) have a vanishing sum and solve a quartic equation without a cubic term,

$$\kappa^4 - A_2 \kappa^2 + A_1 \kappa - A_0 = 0, \quad (27)$$

where

$$\begin{aligned} A_2 &= \frac{1}{2} \text{Tr} \{K^2\}, \\ A_1 &= -\frac{1}{3} \text{Tr} \{K^3\}, \\ A_0 &= \frac{1}{4} \text{Tr} \{K^4\} - \frac{1}{8} [\text{Tr} \{K^2\}]^2. \end{aligned} \quad (28)$$

These three numbers are invariant under arbitrary (local or not) unitary transformations; they are three independent *global* invariants of the given P. Expressed in terms of s^\downarrow , \vec{t} , and \overleftarrow{C} they read

$$\begin{aligned}
A_2 &= 2 \operatorname{Sp} \left\{ \overleftarrow{C}^T \cdot \overleftarrow{C} \right\} + 2(s^2 + t^2), \\
A_1 &= 8 \det \left\{ \overleftarrow{C} \right\} - 8 \vec{s} \cdot \overleftarrow{C} \cdot t^\downarrow, \\
A_0 &= - \left(\frac{1}{2} A_2 \right)^2 + 2 \left[\operatorname{Sp} \left\{ \overleftarrow{C}^T \cdot \overleftarrow{C} \right\} \right]^2 + 4s^2 t^2 \\
&\quad + 4 \vec{s} \cdot \overleftarrow{C} \cdot \overleftarrow{C}^T \cdot s^\downarrow + 4 \vec{t} \cdot \overleftarrow{C}^T \cdot \overleftarrow{C} \cdot t^\downarrow \\
&\quad + 8 \det \left\{ \overleftarrow{E} \right\} - 8 \det \left\{ \overleftarrow{C} \right\}
\end{aligned} \tag{29}$$

where

$$\overleftarrow{E} = \overleftarrow{C} - s^\downarrow \vec{t} \tag{30}$$

is the entanglement dyadic.

As we see, the traces of (28) involve nine different local polynomial invariants of s^\downarrow , \vec{t} , and \overleftarrow{C} , and it is clear that their values are determined by the nine family-specifying parameters of classes A, ..., F. Suggestive as it is, the converse is not true,² as can be demonstrated by a counter example. Consider, for instance, the two states

$$\begin{aligned}
P_1 &= \frac{1}{4} \left(1 + \frac{1}{4} \sigma_1 + \frac{1}{2} \sigma_3 + \frac{1}{2} \sigma_1 \tau_1 + \frac{1}{4} \sigma_2 \tau_2 \right), \\
P_2 &= \frac{1}{4} \left(1 + \frac{1}{2} \sigma_2 + \frac{1}{4} \sigma_3 + \frac{1}{2} \sigma_1 \tau_1 + \frac{1}{4} \sigma_2 \tau_2 \right),
\end{aligned} \tag{31}$$

which belong to two different class-F families, but all terms in (29) are the same for P_1 and P_2 .

Whereas the nine polynomial invariants of (29) do not always suffice to determine the values of all local invariants, the nine parameters that specify the family certainly do. They are, however, not given by (traces of) polynomials of s^\downarrow , \vec{t} , and \overleftarrow{C} . According to Makhlin [9], there are 18 polynomial invariants whose values uniquely characterize the family in question (actually, of nine of them only the sign matters). In addition to the nine invariants in (29), which exhaust the polynomials of degree 4 or lower, there are nine invariants of higher degree in Makhlin's set, which do not enter the three global invariants A_0 , A_1 , A_2 .

All solutions of the quartic equation (27) are real by construction — it is, after all, the characteristic polynomial of a hermitian operator. Then, if all solutions are in the range $\kappa \leq 1$, this polynomial and its derivatives must be non-negative for $\kappa \geq 1$. Consequently, the positivity requirement (24) implies

$$A_2 - A_1 + A_0 \leq 1, \quad 2A_2 - A_1 \leq 4, \quad A_2 \leq 6. \tag{32}$$

²Therefore, the assertion “All other local invariants ...” shortly after (19) in [5] is false.

The converse is also true: If these three inequalities are obeyed, the four real solutions of (27) are in the range $\kappa \leq 1$, so that $K \leq 1$ and $P \geq 0$. In other words, the restrictions on s^\downarrow , \vec{t} , and \overrightarrow{C} alluded to at the beginning of this section are just the inequalities (32).

Although the equivalence of (24) and (32) is rather obvious, a clear-cut demonstration of the case could be of interest to some readers. We give one in the Appendix.

If the entanglement dyadic \overrightarrow{E} vanishes, the state in question is of product form,

$$P = \frac{1}{2} \left(1 + \vec{\sigma} \cdot s^\downarrow \right) \frac{1}{2} \left(1 + \vec{t} \cdot \tau^\downarrow \right), \quad (33)$$

so that results of measurements on the first q-bit show no correlations whatsoever with measurement results concerning the second q-bit. Under these circumstances the 2-q-bit system is *not entangled*. Entangled q-bit pairs, $\overrightarrow{E} \neq 0$, may be in a mixed state blended from disentangled ingredients,

$$P = \sum_n w_n \frac{1}{2} \left(1 + \vec{\sigma} \cdot s_n^\downarrow \right) \frac{1}{2} \left(1 + \vec{t}_n \cdot \tau^\downarrow \right) \\ \text{with } w_n > 0, \sum_n w_n = 1; \quad (34)$$

then all correlations found in the measurement data can be understood classically. States of this kind are called *separable*. As an elementary example, consider the pure states (20): For $p = 1$ they are not entangled and therefore separable, for $p < 1$ they are entangled and not separable.

Correlations of a genuine quantum character require a non-separable state P . According to a criterion that we owe to Peres [10] as well as M., P., and R. Horodecki [11], a given state P is separable if

$$\tilde{P} = \frac{1}{4} \left(1 - \vec{\sigma} \cdot s^\downarrow + \vec{t} \cdot \tau^\downarrow - \vec{\sigma} \cdot \overrightarrow{C} \cdot \tau^\downarrow \right) \\ = \frac{1}{2} \left(\vec{\sigma} \cdot P \sigma^\downarrow - P \right) \quad (35)$$

is positive and only then. Let's call \tilde{P} the PH_3 transform of P ; it is unitarily equivalent to the partial transpose originally considered by Peres and the Horodeckis.

The positivity of \tilde{P} , or

$$1 - 4\tilde{P} = \tilde{K} = \frac{1}{2} \left(\vec{\sigma} \cdot K \sigma^\downarrow - K \right) \leq 1, \quad (36)$$

can be checked analogously to the positivity of P . Now, the quartic equation solved by the eigenvalues $\tilde{\kappa}_1, \dots, \tilde{\kappa}_4$ of \tilde{K} is

$$\tilde{\kappa}^4 - A_2 \tilde{\kappa}^2 + \left(A_1 + 16 \det \left\{ \overrightarrow{C} \right\} \right) \tilde{\kappa} \\ - \left(A_0 - 16 \det \left\{ \overrightarrow{E} \right\} + 16 \det \left\{ \overrightarrow{C} \right\} \right) = 0, \quad (37)$$

so that

$$\begin{aligned}
A_2 - A_1 + A_0 &\leq 1 + 16 \det \left\{ \overleftarrow{E} \right\}, \\
2A_2 - A_1 &\leq 4 + 16 \det \left\{ \overleftarrow{C} \right\}, \\
A_2 &\leq 6.
\end{aligned} \tag{38}$$

are equivalent to (36); the third is always obeyed by a positive P . So, a non-separable state must violate either the first or the second inequality, or both. The equal sign holds in the first inequality, if the PH_3 transform of the given P has a zero eigenvalue; the first and the second are equalities, if the PH_3 transform has two zero eigenvalues. Accordingly, the \tilde{P} of a non-separable P can at most have one zero eigenvalue and thus must be of rank 3 or 4. While we are at it, let us also mention that the PH_3 transform of any state P can have at most a single negative eigenvalue [see below at Eq. (44)].

Thus the separability of a given P is checked as easily as its positivity. Neither test requires actual knowledge of the solutions of (27) or (37). They could, of course, be stated analytically but these explicit expressions are not very transparent unless special relations exist among the coefficients of the quartic equations.

As an immediate implication of the PH_3 criterion, in the form of the inequalities (38), we note that a state P with $\det \left\{ \overleftarrow{C} \right\} \geq 0$ and $\det \left\{ \overleftarrow{E} \right\} \geq 0$ is surely separable. Therefore, for example, all states in classes A and C are separable.

4 Lewenstein-Sanpera decompositions

As Lewenstein and Sanpera observed [4], any 2-q-bit state P can be written as a convex sum of a separable state and a pure state,

$$P = \lambda P_{\text{sep}} + (1 - \lambda) P_{\text{pure}} \quad \text{with} \quad 0 \leq \lambda \leq 1. \tag{39}$$

Rare exceptions aside, the *Lewenstein-Sanpera decomposition* (LSD) of a given (non-separable) P is not unique, there is usually a continuum of LSDs to choose from. Among them is the *optimal LSD*, the one with the largest value of λ ,

$$P = \mathcal{S} P_{\text{sep}}^{(\text{opt})} + (1 - \mathcal{S}) P_{\text{pure}}^{(\text{opt})} \quad \text{with} \quad \mathcal{S} = \max\{\lambda\}, \tag{40}$$

and we call \mathcal{S} , the maximal λ value, the *degree of separability* of P . Without presently attempting to be precise about this matter, we repeat the remark in [5] that “a state P is the more useful for quantum communication purposes, the smaller its degree of separability.”

The spectral decomposition of the PH_3 transform of a pure state (20) is of the generic form

$$\tilde{P}_{\text{pure}} = \frac{1}{4} (1 - p\sigma_1 - p\tau_1 + \sigma_1\tau_1 + q\sigma_2\tau_2 + q\sigma_3\tau_3)$$

$$= \frac{1+p}{2} P_{\text{pure}}^{(1)} + \frac{1-p}{2} P_{\text{pure}}^{(2)} + \frac{q}{2} P_{\text{pure}}^{(3)} - \frac{q}{2} P_{\text{pure}}^{(4)} \quad (41)$$

with

$$\left. \begin{array}{l} P_{\text{pure}}^{(1)} \\ P_{\text{pure}}^{(2)} \end{array} \right\} = \frac{1}{4} (1 \mp \sigma_1 \mp \tau_1 + \sigma_1 \tau_1) , \quad (42)$$

which are pure states of the separable class-C kind, and

$$\left. \begin{array}{l} P_{\text{pure}}^{(3)} \\ P_{\text{pure}}^{(4)} \end{array} \right\} = \frac{1}{4} (1 - \sigma_1 \tau_1 \pm \sigma_2 \tau_2 \pm \sigma_3 \tau_3) , \quad (43)$$

which are Bell states (non-separable, class B). Therefore, the PH_3 transform \tilde{P} of any 2-q-bit state P can be written as

$$\tilde{P} = (1+x)P' - xP_{\text{Bell}} , \quad 0 \leq x \leq \frac{1}{2}(1-\mathcal{S}) \quad (44)$$

with some state P' and a Bell state P_{Bell} . As a consequence, \tilde{P} can have at most one negative eigenvalue, so that only one solution of (37) can be in the range $\tilde{\kappa} > 1$, as noted above.

Since P' is a mixture of four or fewer pure states, (44) shows that the PH_3 transform of a non-separable state is a pseudo-mixture of up to five pure states with one negative weight only, carried by a Bell state. There is a very similar observation by Sanpera, Tarrach, and Vidal [12] about P itself: It can always be presented as a pseudo-mixture of four or five separable pure states; as an immediate consequence its PH_3 transform is also such a pseudo-mixture.

The optimal LSD (40) has a number of properties that help in decomposing given states in the optimal way. Let's briefly consider some particularly important ones.

Existence: The degree of separability \mathcal{S} is really the maximum of all possible λ values in (39), not just their supremum, because the subset of separable states is compact. Therefore, a LSD with $\lambda = \mathcal{S}$ does exist.

Uniqueness: If we have two different LSDs with the same non-zero value of λ , their symmetric convex sum also equals the given P . It contains the convex sum of the two different P_{sep} s, which is separable, and the convex sum of the two P_{pure} s, which has LSDs of its own. Either one of them contains a separable part, so that we get a new LSD of the P in question with a larger λ value. Consequently, the common λ of the original two LSDs is not maximal, and it follows that the optimal LSD is unique.

This does not imply that one can always find another LSD with the same λ value if $\lambda < \mathcal{S}$. There are P s with a continuum of LSDs in which each value of λ occurs only once.³ Examples are the rank-2 states of (56) in [5] that obey inequality (61) in [5].

³Therefore, the 'only' is too strong in the assertion "Only P_{sep} and P_{pure} ..." after (15) in [5].

$P_{\text{sep}}^{(\text{opt})}$ **is barely separable:** Consider the optimal LSD of some non-separable P and a parameter ϵ in the range $0 < \epsilon \leq 1 - \mathcal{S}$. In

$$P = (\mathcal{S} + \epsilon) \left[\frac{\mathcal{S}}{\mathcal{S} + \epsilon} P_{\text{sep}}^{(\text{opt})} + \frac{\epsilon}{\mathcal{S} + \epsilon} P_{\text{pure}}^{(\text{opt})} \right] + (1 - \mathcal{S} - \epsilon) P_{\text{pure}}^{(\text{opt})} \quad (45)$$

the convex sum in square brackets is surely non-negative, but cannot be separable. Because, if it were, we would have found a LSD with $\lambda > \mathcal{S}$. Thus the PH_3 transform of $[\dots]$ has a negative eigenvalue for $\epsilon > 0$, but none for $\epsilon = 0$. Since the eigenvalues are continuous functions of ϵ , the PH_3 transform of $P_{\text{sep}}^{(\text{opt})}$ must have at least one zero eigenvalue. Formally,

$$\tilde{P}_{\text{sep}}^{(\text{opt})} \geq 0 \quad \text{but not} \quad \tilde{P}_{\text{sep}}^{(\text{opt})} > 0; \quad (46)$$

for $P_{\text{sep}}^{(\text{opt})}$, the equal sign holds in the first inequality of (38). A useful terminology calls $P_{\text{sep}}^{(\text{opt})}$ *barely separable* with respect to $P_{\text{pure}}^{(\text{opt})}$.

When searching for the optimal LSD of a given P it is, therefore, sufficient to consider LSDs with P_{sep} s that are barely separable with respect to the P_{pure} with which they are paired in (39). If the P_{sep} of some LSD does not have this property, one adds the appropriate amount of the respective P_{pure} to it (in the sense of a convex sum, of course) and gets a barely separable P_{sep} .

Local invariance is passed on: Suppose that the P considered is invariant under some local unitary transformation,

$$U_{\text{loc}}^\dagger P U_{\text{loc}} = P. \quad (47)$$

Then its $P_{\text{sep}}^{(\text{opt})}$ and $P_{\text{pure}}^{(\text{opt})}$ must be invariant under this local transformation as well. Otherwise we could apply it to the optimal LSD and get another LSD with the same λ value, in conflict with the uniqueness of the optimal LSD. This argument builds on the elementary observation that local transformations do not affect the purity and separability of a state.

The limitations resulting from this “inheritance of local invariance” can facilitate the search for the optimal LSD substantially. The optimal decompositions of the (generalized) Werner states reported in [5] were found this way.

Swapping invariance is passed on: Similarly one finds that the $P_{\text{sep}}^{(\text{opt})}$ and $P_{\text{pure}}^{(\text{opt})}$ of a P that is invariant under the swapping transformation

$$\sigma_k \leftrightarrow \tau_k \quad \text{for} \quad k = 1, 2, 3 \quad (48)$$

must be invariant themselves because swapping does not affect the separability or the purity of a state. Clearly, this swapping invariance is only possible if the Pauli vectors s^\downarrow and \vec{t} are of equal length.

Orthogonality is passed on: If the P in question is orthogonal to a certain other state P_\perp ,

$$\text{Tr}\{PP_\perp\} = 0, \quad (49)$$

then the P_{sep} s and P_{pure} s of all LSDs of P are also orthogonal to P_{\perp} because both traces in

$$0 = \lambda \text{Tr} \{P_{\text{sep}} P_{\perp}\} + (1 - \lambda) \text{Tr} \{P_{\text{pure}} P_{\perp}\} \quad (50)$$

must be non-negative, so both must vanish. In particular, the $P_{\text{sep}}^{(\text{opt})}$ and $P_{\text{pure}}^{(\text{opt})}$ of P must have this orthogonality property. The optimal LSDs of rank-2 states reported in [5] were found by exploiting this “inheritance of orthogonality.”

5 Degree of separability and concurrence

In their studies of what they call “entanglement of formation,” Hill and Wootters [6, 7] consider

$$\begin{aligned} \bar{P} &= \frac{1}{4} \left(1 - \vec{\sigma} \cdot s^{\downarrow} - \vec{t} \cdot \tau^{\downarrow} + \vec{\sigma} \cdot \vec{C} \cdot \tau^{\downarrow} \right) \\ &= \frac{1}{2} \left(\vec{\tau} \cdot \tilde{P} \tau^{\downarrow} - \tilde{P} \right); \end{aligned} \quad (51)$$

let’s call it the HW transform of P . Since the replacement $(s^{\downarrow}, \vec{t}, \vec{C}) \rightarrow (-s^{\downarrow}, -\vec{t}, \vec{C})$ changes none of the local invariants in (29), \bar{P} has the same eigenvalues as P and, therefore, \bar{P} is unitarily equivalent to P . Equally well we could argue that the matrix representations of P and \bar{P} , composed of the ingredients in (25) and (26), are complex conjugates or transposes of each other, and so they must have the same real eigenvalues. Note that a 2-q-bit state and its HW transform are always in the same class of states but they may or may not belong to the same family; their unitary equivalence may be local or global.

Hill and Wootters use the HW transform to introduce the *concurrence* \mathcal{C} of P . It is given by

$$\mathcal{C} = \max \left\{ 0, 2 \max_k \{r_k\} - \sum_k r_k \right\}, \quad (52)$$

where r_1, r_2, r_3, r_4 are the four non-negative eigenvalues of

$$\left| \sqrt{P} \sqrt{\bar{P}} \right| = \sqrt{\sqrt{\bar{P}} P \sqrt{\bar{P}}}. \quad (53)$$

The roles of P and \bar{P} can be interchanged in this definition of \mathcal{C} ; thus the concurrence of \bar{P} is equal to the concurrence of P . For instance, the concurrence of a pure state (20) is q .

Separable states ($\mathcal{S} = 1$) have $\mathcal{C} = 0$ and non-separable states ($\mathcal{S} < 1$) have $\mathcal{C} > 0$. This suggests that there might be a close relation between the degree of separability and the concurrence. Indeed, $\mathcal{S} + \mathcal{C} = 1$ holds if $s^{\downarrow} = 0$ and $\vec{t} = 0$ — such P s are generalized Werner states of the first kind in the terminology of [5] — but more generally we find

$$0 < \mathcal{S} + \mathcal{C} \leq 1. \quad (54)$$

Pure states (20) have $\mathcal{S} + \mathcal{C} = 1$ if $q = 0$ and $\mathcal{S} + \mathcal{C} = q$ if $q > 0$. A set of non-pure states exploring the whole range of (54) is given by the rank-2 states

$$P = \frac{1}{4} \left(1 + (\sigma_3 + x\tau_3) \sin \theta + (\sigma_1\tau_1 - x\sigma_2\tau_2) \cos \theta + x\sigma_3\tau_3 \right) \quad (55)$$

with $-1 < x < 1$, for which

$$\mathcal{S} = \begin{cases} 1 & \text{if } \cos \theta = 0 \\ 1 - |x| & \text{if } \cos \theta \neq 0 \end{cases}, \quad \mathcal{C} = |x \cos \theta|. \quad (56)$$

We surmise that (54) is obeyed by all 2-q-bit states.

Appendix

We write the four solutions of (27) in terms of three parameters,

$$\begin{aligned} \begin{Bmatrix} \kappa_1 \\ \kappa_2 \end{Bmatrix} &= \pm(\lambda_1 - \lambda_2) - \lambda_3, \\ \begin{Bmatrix} \kappa_3 \\ \kappa_4 \end{Bmatrix} &= \mp(\lambda_1 + \lambda_2) + \lambda_3, \end{aligned} \quad (57)$$

thereby taking care of $\text{Tr}\{K\} = \kappa_1 + \kappa_2 + \kappa_3 + \kappa_4 = 0$. The coefficients in (27) are then given by

$$\begin{aligned} A_2 &= \frac{1}{2} (\kappa_1^2 + \kappa_2^2 + \kappa_3^2 + \kappa_4^2) \\ &= 2 (\lambda_1^2 + \lambda_2^2 + \lambda_3^2), \\ A_1 &= \kappa_1\kappa_2(\kappa_1 + \kappa_2) + \kappa_3\kappa_4(\kappa_3 + \kappa_4) \\ &= -8\lambda_1\lambda_2\lambda_3, \\ A_0 &= -\kappa_1\kappa_2\kappa_3\kappa_4 = 2 (\lambda_1^2\lambda_2^2 + \lambda_2^2\lambda_3^2 + \lambda_3^2\lambda_1^2) \\ &\quad - (\lambda_1^4 + \lambda_2^4 + \lambda_3^4). \end{aligned} \quad (58)$$

Now look at the second inequality in (32). It says

$$\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + 2\lambda_1\lambda_2\lambda_3 \leq 1 \quad (59)$$

or, singling out λ_3 ,

$$(\lambda_1\lambda_2 + \lambda_3)^2 \leq (1 - \lambda_1^2)(1 - \lambda_2^2), \quad (60)$$

and cyclic permutations produce two analogous statements in which λ_1 and λ_2 are privileged. Since the left-hand sides of these three equations are non-negative, it follows that all λ_j^2 exceed unity if one of them does. Combined with the third inequality in (32), here reading

$$\lambda_1^2 + \lambda_2^2 + \lambda_3^2 \leq 3, \quad (61)$$

this implies

$$\lambda_1^2 \leq 1, \quad \lambda_2^2 \leq 1, \quad \lambda_3^2 \leq 1. \quad (62)$$

In conjunction with

$$\begin{aligned} \lambda_1 &= \frac{1}{2}(\kappa_1 + \kappa_4) = -\frac{1}{2}(\kappa_2 + \kappa_3), \\ \lambda_2 &= \frac{1}{2}(\kappa_2 + \kappa_4) = -\frac{1}{2}(\kappa_1 + \kappa_3), \\ \lambda_3 &= \frac{1}{2}(\kappa_3 + \kappa_4) = -\frac{1}{2}(\kappa_1 + \kappa_2) \end{aligned} \quad (63)$$

this means that at most one of the four κ s can be larger than 1, and that then the other three must be less than 1. But the first inequality in (32),

$$1 - A_2 + A_1 - A_0 = (1 - \kappa_1)(1 - \kappa_2)(1 - \kappa_3)(1 - \kappa_4) \geq 0, \quad (64)$$

excludes this possibility because one negative factor and three positive factors would yield a negative product. Therefore, all three inequalities (32) can only be obeyed if all four κ s are less than 1. In other words: (32) implies (24) indeed.

Note that this reasoning is only valid if one knows, as we do, that all solutions of the quartic equation (27) are real. This property itself is not guaranteed by the inequalities (32), as shown by $A_2 = 2$, $A_1 = 0$, $A_0 = -2$ when $(\kappa^2 - 1)^2 + 1 = 0$.

Acknowledgments

BGE thanks Marek Kuś, Maciej Lewenstein, and Karol Życzkowski for particularly helpful discussions. NM would like to thank the Egyptian government for granting a fellowship.

References

- [1] W. K. Wootters, B. D. Fields: *Ann. Phys. (NY)* **191**, 363–381 (1989).
- [2] Č. Brukner, A. Zeilinger: *Phys. Rev. Lett.* **83**, 3354–3357 (1999).
- [3] B.-G. Englert, Ch. Kurtsiefer, H. Weinfurter: *Phys. Rev. A* (submitted).
- [4] M. Lewenstein, A. Sanpera: *Phys. Rev. Lett.* **80**, 2261–2264 (1998).
- [5] B.-G. Englert, N. Metwally: *J. Mod. Opt.*, in print (LANL preprint quant-ph/9912089).
- [6] S. Hill, W. K. Wootters: *Phys. Rev. Lett.* **78**, 5022–5025 (1997).
- [7] W. K. Wootters: *Phys. Rev. Lett.* **80**, 2245–2248 (1998).
- [8] M. Kuś, K. Życzkowski:
LANL preprint quant-ph/0006068.
- [9] Y. Makhlin: LANL preprint quant-ph/0002045.

- [10] A. Peres: Phys. Rev. Lett. **77**, 1413–1415 (1996).
- [11] M. Horodecki, P. Horodecki, R. Horodecki: Phys. Lett. **A223**, 1–8 (1996).
- [12] A. Sanpera, R. Tarrach, G. Vidal: Phys. Rev. A **58**, 826–830 (1998).

This paper has been submitted to
Applied Physics B
as a contribution to the
Proceedings of the DPG Spring Meeting,
held in Bonn, April 2000.